คู่มือการใช้งาน OpenVas (Greenbone)

Step การใช้งาน OpenVas (Greenbone)

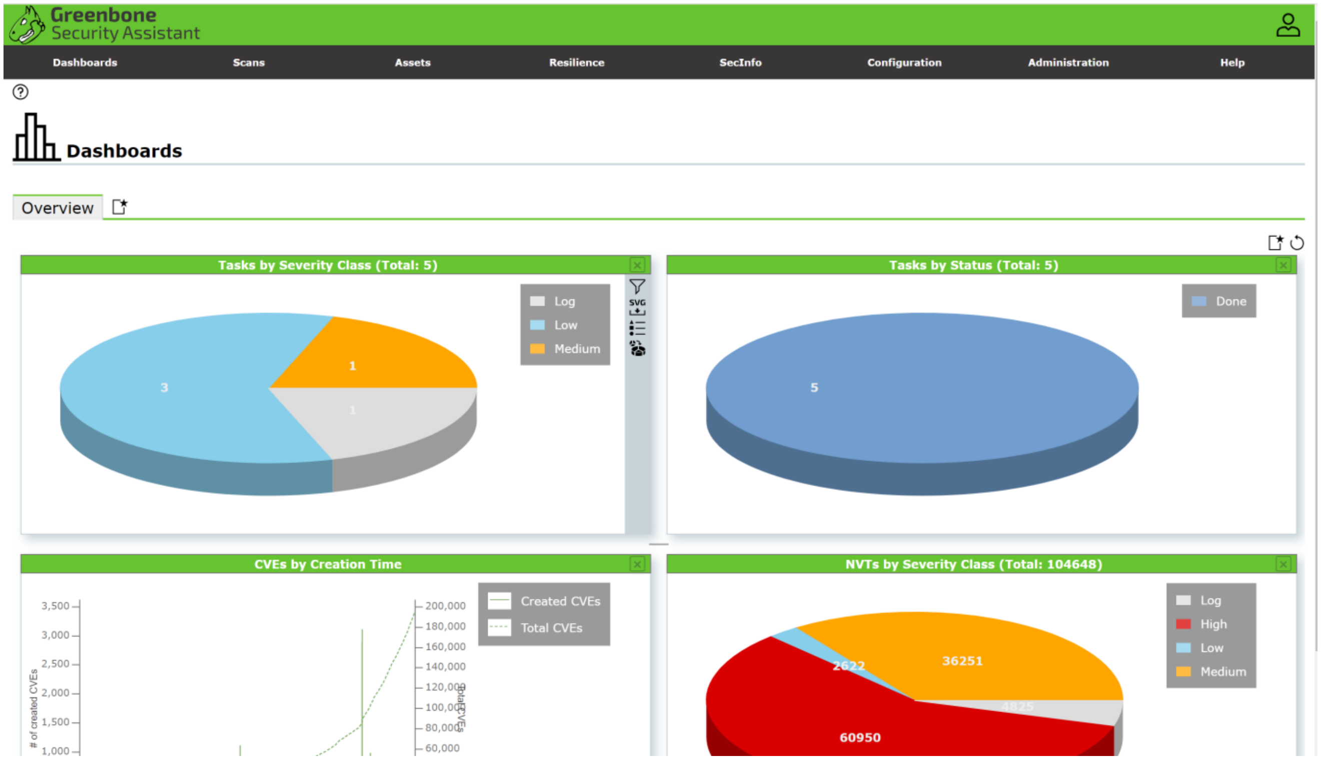
Step 1. ตรวจสอบ Version ของ OpenVas ว่า update ล่าสุดแล้วหรือยัง

Step 2. ทำการสร้าง Targets (สามารถสร้าง Credentials ได้)

Step 3. ทำการสร้าง Tasks และสั่ง Scan (สามารถตั้ง Schedule ในการ Scan ได้)

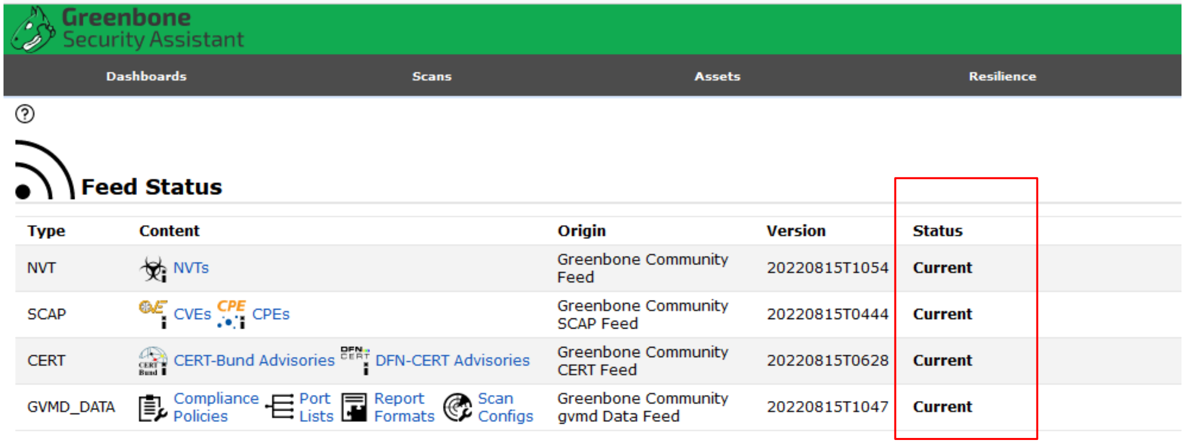
Step 4. เมื่อทำการ Scan เสร็จทำการตรวจสอบผลการ Scan

1. เข้าใช้งานระบบ OpenVas (Greenbone) ผ่าน URL : https://164.115.35.18:9392/ และทำการ Login ด้วย Username Password ที่ทางทีมทำการส่งให้



2. ทำการตรวจสอบ Version

2.1 เลือกเมนู Administration > Feed Status



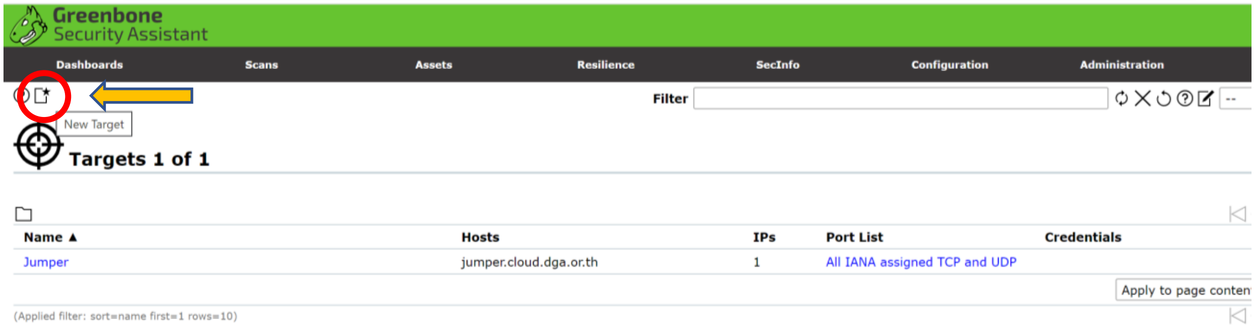
Feed Status

Type	Content	Origin	Version	Status
NVT	NVTs	Greenbone Community Feed	20220815T1054	**Current**
SCAP	CVEs CPEs	Greenbone Community SCAP Feed	20220815T0444	**Current**
CERT	CERT-Bund Advisories DFN-CERT Advisories	Greenbone Community CERT Feed	20220815T0628	**Current**
GVMD_DATA	Compliance Policies Port Lists Report Formats Scan Configs	Greenbone Community gvmd Data Feed	20220815T1047	**Current**

ปล. หาก Status มีการ Update ไปมากกว่า 7 วันให้ทำการแจ้ง Admin

3. ทำการสร้าง Targets

3.1 Configuration > Targets > เลือก New Target

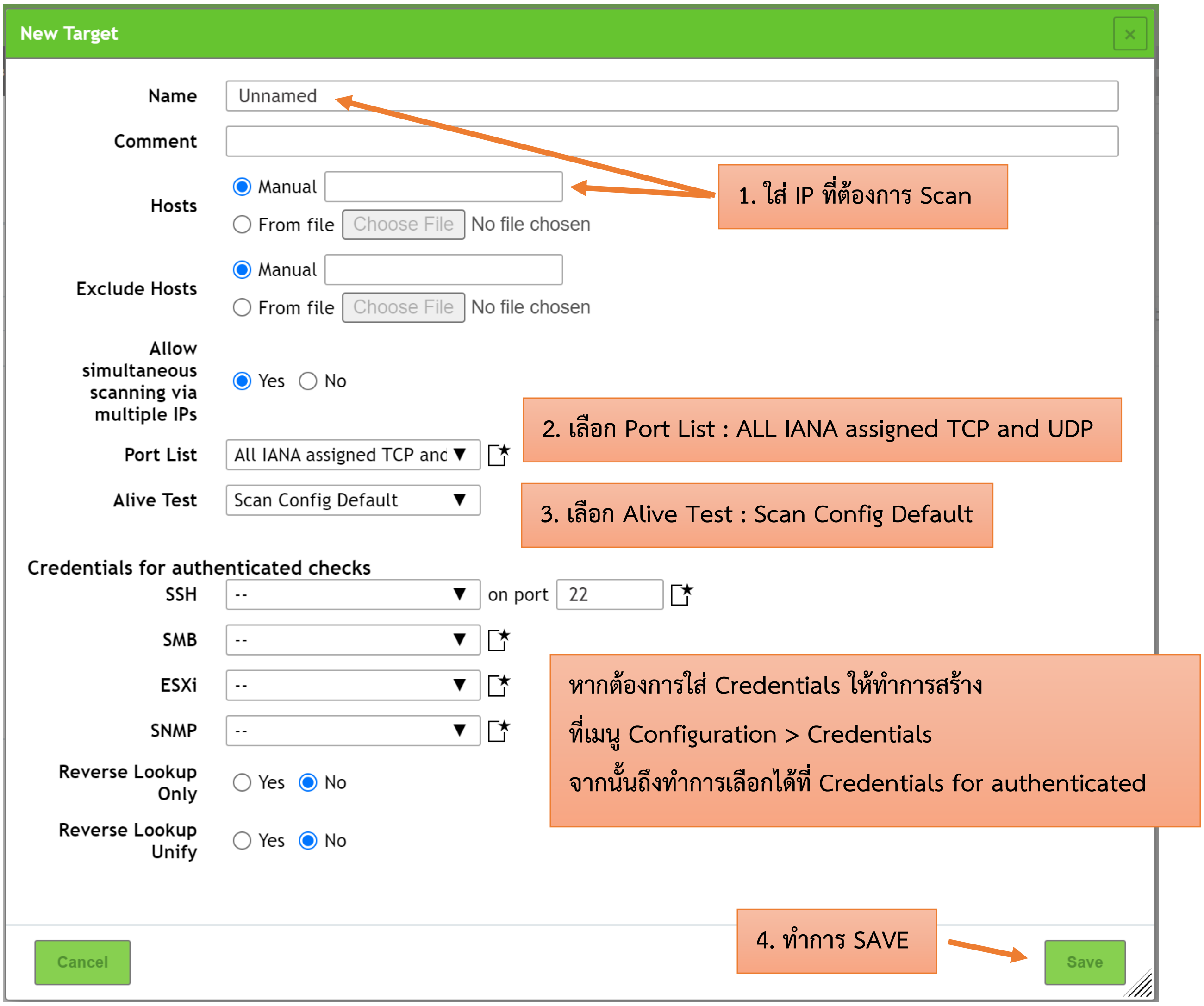


Targets 1 of 1

Name ▲	Hosts	IPs	Port List	Credentials
Jumper	jumper.cloud.dga.or.th	1	All IANA assigned TCP and UDP	

(Applied filter: sort=name first=1 rows=10)

3.2 ทำการกรอก IP ที่ต้องการ Scan



New Target

Name	Unnamed
Comment	
Hosts	● Manual ␣ ○ From file Choose File No file chosen
Exclude Hosts	● Manual ○ From file Choose File No file chosen
Allow simultaneous scanning via multiple IPs	● Yes ○ No
Port List	All IANA assigned TCP anc ▼
Alive Test	Scan Config Default ▼

Credentials for authenticated checks

SSH	-- ▼ on port 22
SMB	-- ▼
ESXi	-- ▼
SNMP	-- ▼
Reverse Lookup Only	○ Yes ● No
Reverse Lookup Unify	○ Yes ● No

1. ใส่ IP ที่ต้องการ Scan

2. เลือก Port List : ALL IANA assigned TCP and UDP

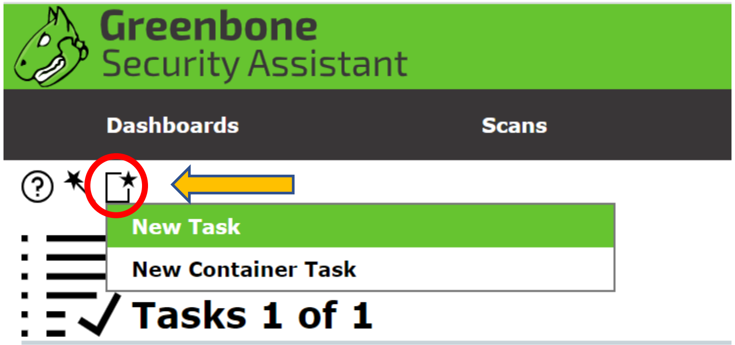
3. เลือก Alive Test : Scan Config Default

หากต้องการใส่ Credentials ให้ทำการสร้าง
ที่เมนู Configuration > Credentials
จากนั้นถึงทำการเลือกได้ที่ Credentials for authenticated

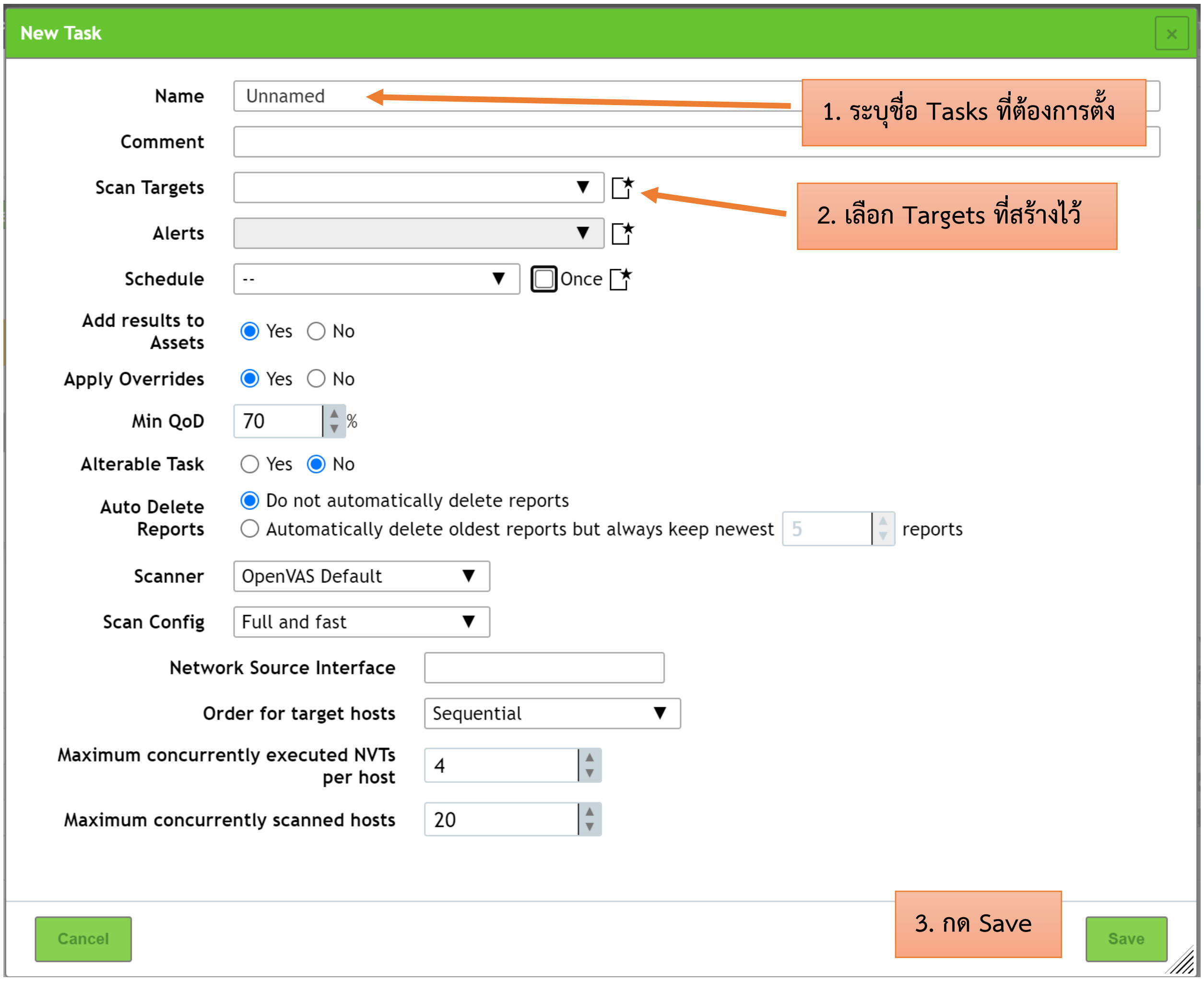
4. ทำการ SAVE

4. ทำการสร้าง Tasks และสั่ง Scan

4.1 เลือกเมนู Scans > Tasks > เลือก New Task



4.2 ทำการเลือก Target ที่ได้สร้างไว้ และกรอกข้อมูลการ Scan เพิ่มเติม



New Task

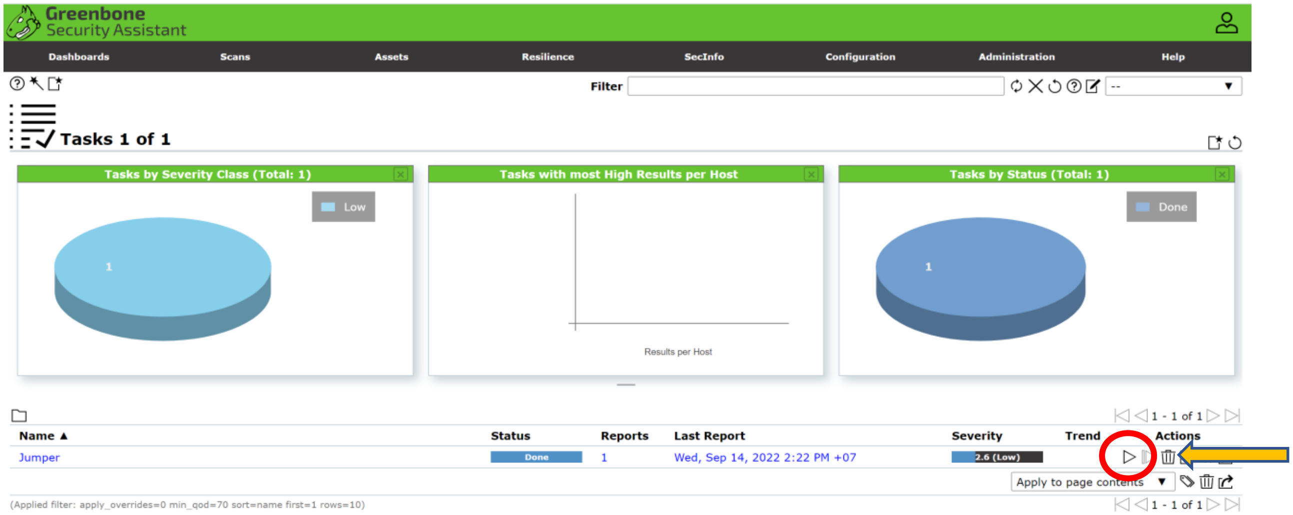
Name	Unnamed
Comment	
Scan Targets	▼
Alerts	▼
Schedule	-- ▼ □ Once
Add results to Assets	● Yes ○ No
Apply Overrides	● Yes ○ No
Min QoD	70 %
Alterable Task	○ Yes ● No
Auto Delete Reports	● Do not automatically delete reports ○ Automatically delete oldest reports but always keep newest 5 reports
Scanner	OpenVAS Default ▼
Scan Config	Full and fast ▼
Network Source Interface	
Order for target hosts	Sequential ▼
Maximum concurrently executed NVTs per host	4
Maximum concurrently scanned hosts	20

1. ระบุชื่อ Tasks ที่ต้องการตั้ง

2. เลือก Targets ที่สร้างไว้

3. กด Save

4.3 ทำการ Scan ทันที



Tasks 1 of 1

1 - 1 of 1

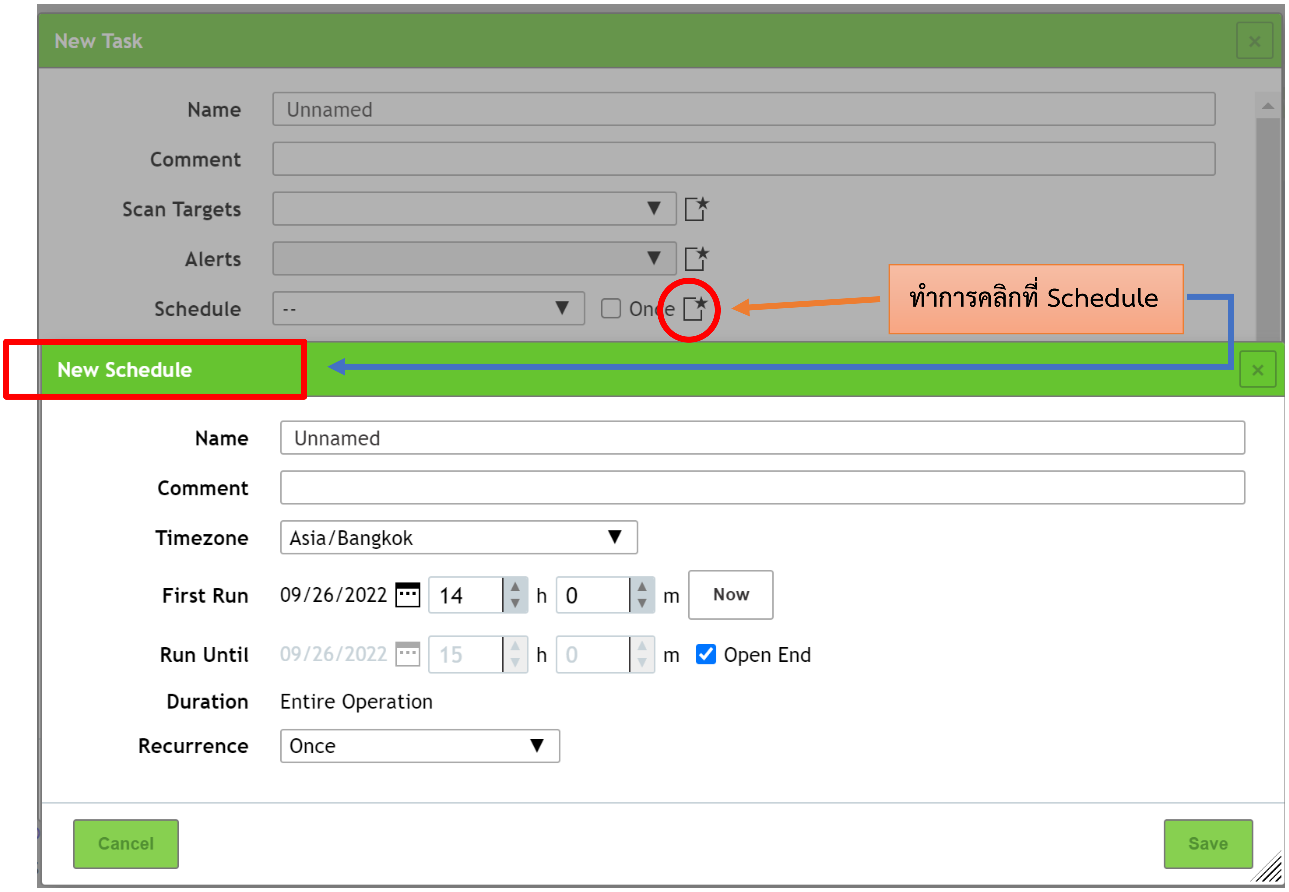
Name ▲	Status	Reports	Last Report	Severity	Trend	Actions
Jumper	Done	1	Wed, Sep 14, 2022 2:22 PM +07	2.6 (Low)		

Apply to page contents ▼

(Applied filter: apply_overrides=0 min_qod=70 sort=name first=1 rows=10)

1 - 1 of 1

4.4 ทำการตั้ง Schedule ในการ Scan



New Task

Name: Unnamed

Comment:

Scan Targets:

Alerts:

Schedule: -- □ Once

ทำการคลิกที่ Schedule

New Schedule

Name: Unnamed

Comment:

Timezone: Asia/Bangkok

First Run: 09/26/2022 14 h 0 m Now

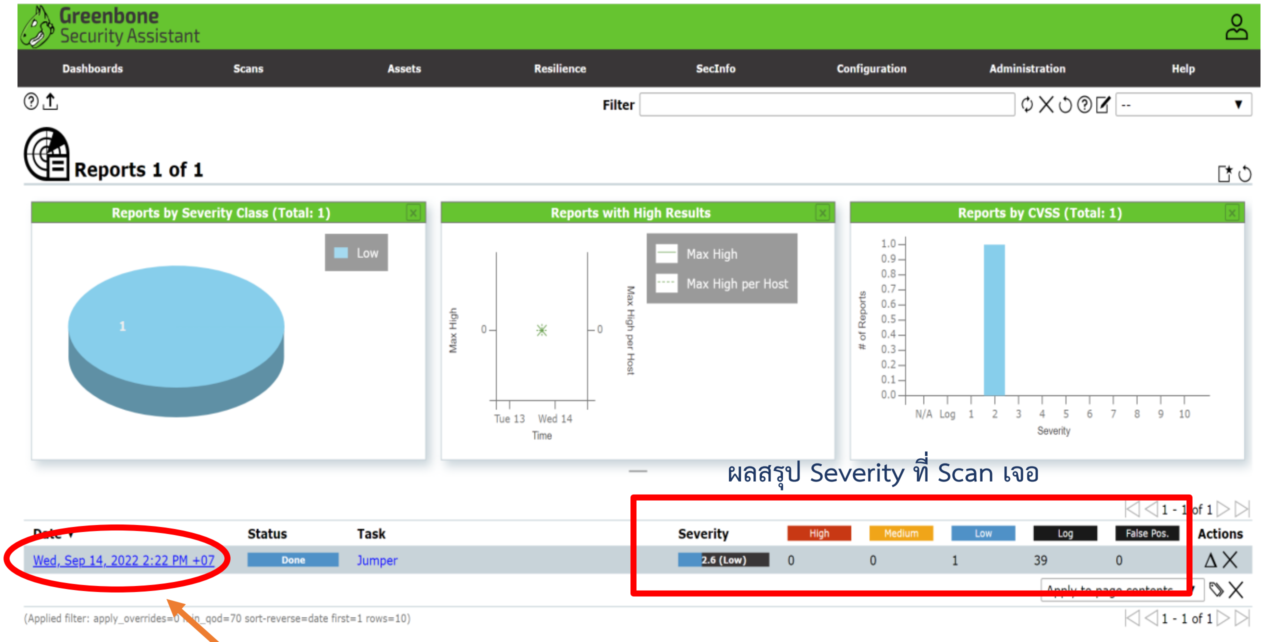
Run Until: 09/26/2022 15 h 0 m ☑ Open End

Duration: Entire Operation

Recurrence: Once

5. ตรวจสอบผลการ Scan

5.1 เลือกเมนู Scans > Reports



Reports 1 of 1

ผลสรุป Severity ที่ Scan เจอ

1 - 1 of 1

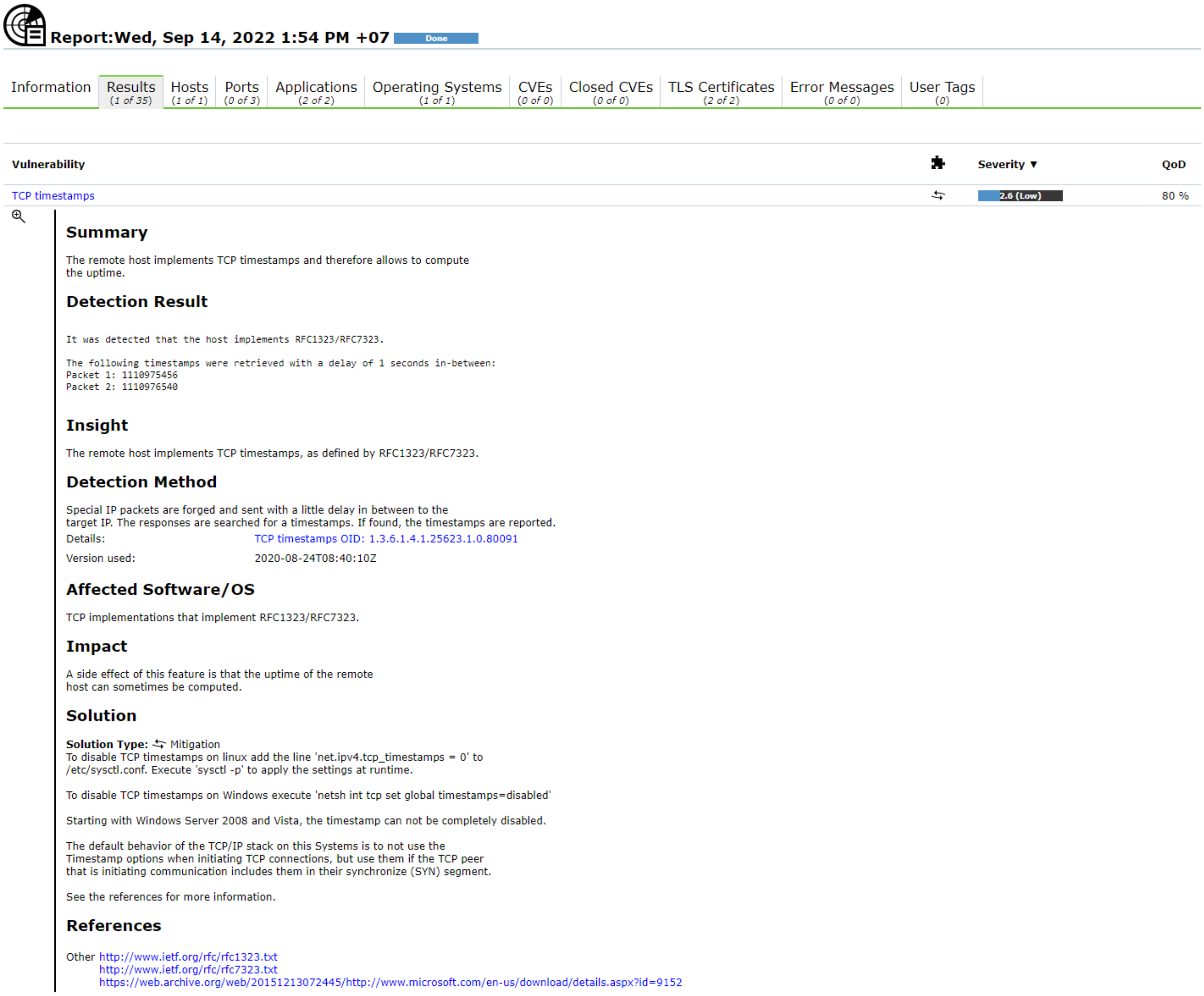
Date ▼	Status	Task	Severity	High	Medium	Low	Log	False Pos.	Actions
Wed, Sep 14, 2022 2:22 PM +07	Done	Jumper	2.6 (Low)	0	0	1	39	0	Δ ✕

(Applied filter: apply_overrides=0 min_qod=70 sort-reverse=date first=1 rows=10)

1 - 1 of 1

คลิกเพื่อดูรายละเอียดเพิ่มเติม

5.2 เลือกที่ Results



Report:Wed, Sep 14, 2022 1:54 PM +07 Done

Information	Results	Hosts	Ports	Applications	Operating Systems	CVEs	Closed CVEs	TLS Certificates	Error Messages	User Tags
	(1 of 35)	(1 of 1)	(0 of 3)	(2 of 2)	(1 of 1)	(0 of 0)	(0 of 0)	(2 of 2)	(0 of 0)	(0)

Vulnerability		Severity ▼	QoD
TCP timestamps	⇆	2.6 (Low)	80 %

Summary

The remote host implements TCP timestamps and therefore allows to compute the uptime.

Detection Result

```
It was detected that the host implements RFC1323/RFC7323.

The following timestamps were retrieved with a delay of 1 seconds in-between:
Packet 1: 1110975456
Packet 2: 1110976540
```

Insight

The remote host implements TCP timestamps, as defined by RFC1323/RFC7323.

Detection Method

Special IP packets are forged and sent with a little delay in between to the target IP. The responses are searched for a timestamps. If found, the timestamps are reported.

Details:	TCP timestamps OID: 1.3.6.1.4.1.25623.1.0.80091
Version used:	2020-08-24T08:40:10Z

Affected Software/OS

TCP implementations that implement RFC1323/RFC7323.

Impact

A side effect of this feature is that the uptime of the remote host can sometimes be computed.

Solution

Solution Type: ⇆ Mitigation
To disable TCP timestamps on linux add the line 'net.ipv4.tcp_timestamps = 0' to /etc/sysctl.conf. Execute 'sysctl -p' to apply the settings at runtime.

To disable TCP timestamps on Windows execute 'netsh int tcp set global timestamps=disabled'

Starting with Windows Server 2008 and Vista, the timestamp can not be completely disabled.

The default behavior of the TCP/IP stack on this Systems is to not use the Timestamp options when initiating TCP connections, but use them if the TCP peer that is initiating communication includes them in their synchronize (SYN) segment.

See the references for more information.

References

Other http://www.ietf.org/rfc/rfc1323.txt
http://www.ietf.org/rfc/rfc7323.txt
https://web.archive.org/web/20151213072445/http://www.microsoft.com/en-us/download/details.aspx?id=9152